PERFORMANCE AUDIT
OF THE

AUTOMATED INFORMATION SYSTEMS

DEPARTMENT OF TREASURY

June 2003

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Automated Information Systems

Department of Treasury

Report Number:
27-590-01

Released:
June 2003

The Department of Treasury has developed and operates large complex information systems to manage the processing of numerous personal and business-related taxes. These include sales, use, and withholding taxes; individual income tax payments and refunds; and single business tax payments and refunds. These information systems facilitate the processing of over $18 billion a year in tax revenue collections and over $1 billion in tax refund payments.

Audit Objective:

To assess the effectiveness of the Department's general controls over access to its mainframe information systems.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Conclusion:

The Department's general controls over access to its mainframe information systems were not effective. As a result, there was a significant risk that the Department's system of internal control could not prevent or detect unauthorized access to or use of confidential taxpayer information or the execution of fraudulent financial transactions.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Post-Fieldwork Follow-Up:

In January 2003, we inquired of the Department and the Department of Information Technology (DIT) their status in addressing the findings in this report. Based on these inquiries, we determined that the Department and DIT had made improvements in the internal control over information systems; however, action was still required to fully correct the conditions cited in the report. The Department and DIT expect to be in full compliance by September 30, 2003.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

The agency preliminary responses indicated that the Department agreed with the findings and has partially complied or will comply with the corresponding recommendations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Material Conditions:

1. Comprehensive Information Systems Security Program

   The Department had not established a comprehensive information systems security program. Without a comprehensive security program, management cannot ensure that the Department's internal control is operating as intended and that sensitive information will remain confidential. (Finding 1)

2. Organizational Controls
   The Department had not established effective organizational controls to support its critical information systems. During our audit, we noted that the cause of many of our audit findings were in part related to incompatible job assignments, critical functions not assigned, or insufficient expertise in control standards and techniques and information security. (Finding 2)

3. Access to System Account
   The Department had not controlled access to its critical production system account. Access to the production system account can be used to gain unauthorized access to critical Department information resources that may go undetected. (Finding 3)

4. Access to Department Information System Files
   The Department had not established effective access controls to its mainframe information system files. The Department stores thousands of files on the State's mainframe computer system. These files support the Department's major tax systems as well as financial and other information systems. We reviewed the access controls for these files and identified material control conditions that prevent the Department from maintaining the integrity and confidentiality of its information systems. (Finding 4)

5. Access to Tax Systems
   The Department had not established effective access controls to its production tax and other information systems. Without effective access control to production application systems, the Department cannot maintain the integrity of confidential taxpayer records and critical financial records. (Finding 5)

6. Program and Data Change Controls
   The Department had not established effective program and data change controls. This environment does not provide Department management with sufficient control to reduce the risk of unauthorized data changes to a reasonable level. (Finding 6)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at:
www.state.mi.us/audgen/

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

James S. Neubecker, C.P.A., C.I.A., D.P.A.
Executive Deputy Auditor General

Scott M. Strong, C.P.A., C.I.A.
Director of Audit Operations

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

June 5, 2003

Mr. Jay B. Rising
State Treasurer
Treasury Building
Lansing, Michigan

Dear Mr. Rising:

This is our report on the performance audit of the Automated Information Systems, Department of Treasury.

This report contains our report summary; description of agency; audit objective, scope, and methodology and agency responses and prior audit follow-up; comment, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This page left intentionally blank.

TABLE OF CONTENTS

AUTOMATED INFORMATION SYSTEMS
DEPARTMENT OF TREASURY

Description of Agency

Information Technology Services Division

The Information Technology Services Division (ITSD) is an organizational component of the Bureau of Administrative Services, Department of Treasury. ITSD's function is to develop, implement, and operate the Department's automated information systems and to provide assistance with these functions. ITSD also provides end-user computing, computer programming, data entry, and mainframe scheduling services to the Department as well as administering the Department's local area network.

The Department has developed and operates large complex information systems to manage the processing of numerous personal and business-related taxes. These include sales, use, and withholding taxes; individual income tax payments and refunds; and single business tax payments and refunds. The Department's information systems facilitate the processing of over $18 billion a year in tax revenue collections and over $1 billion in tax refund payments.

For fiscal year 2000-01, ITSD had appropriations of approximately $12 million and was authorized 171 full-time equated positions.

Subsequent to the completion of our audit fieldwork and effective October 14, 2001, Executive Order No. 2001-3 established the Department of Information Technology (DIT). Within the executive order, all authority, powers, duties, functions, and responsibilities of ITSD were transferred from the Department of Treasury to DIT.

Data Center Operations

Executive Order No. 2001-03 also transferred all authority, powers, duties, functions, and responsibilities of the Data Center Operations* (DCO) from the Department of Management and Budget to DIT.

DCO is responsible for providing centralized data processing services for all State agencies. These services include operational and technical support for a variety of mainframes and services. DCO provides agencies with a complex security system to control access to mainframe resources. DCO's security system allows agency security

** See glossary at end of report for definition.*

administrators to define authorized individuals and grant appropriate access to information resources. It also allows the security administrator to delegate certain security functions to other department employees.

Taxpayer Bill of Rights

Michigan Administrative Code R 205.1003, which is part of the Taxpayer Bill of Rights, states that access to confidential information shall be restricted to Department of Treasury employees who have a need to access the information to perform their duties. A Department employee shall not disclose confidential information to another Department employee, except as needed to perform their duties.

The Taxpayer Bill of Rights (*Michigan Administrative Code* R 205.1007) creates the authority of a disclosure officer for the Department. The disclosure officer is responsible for the development of security directives and the periodic review of security procedures within the Department. Division administrators who have primary custody or control of returns or tax return information are required to determine that the necessary safeguards are in place to prevent the unauthorized use or disclosure of State or federal tax information. It is the responsibility of the Department to issue appropriate written instructions to employees and adopt measures to ensure that employees remain thoroughly familiar with, and strictly adhere to, the rules and procedures governing confidentiality and the disclosure of tax information.

All new Department employees are required to review the policies, procedures, and bulletins governing confidentiality and the authorized disclosure of confidential information and to certify that they are familiar with the documents as the documents relate to the employees specific duties. Periodically, Department employees are required to review the policies, procedures, and bulletins associated with confidential information in the performance of their duties. It is the responsibility of the disclosure officer to annually remind Department employees of the confidentiality requirements.

Internal Audit

The Department assigned its internal auditor the primary responsibility for administering the Department's information security program. DCO's security system allows the security administrator to delegate certain security functions to other Department employees. The Department security administrator can limit an individual's access to tax systems at the level needed to perform the employee's job, as required by the Taxpayer Bill of Rights.

As of October 2000, the Department had established approximately 1,240 individual accounts with access to Department information systems.

Audit Objective, Scope, and Methodology and Agency Responses and Prior Audit Follow-Up

Audit Objective

The objective of our performance audit* of the Automated Information Systems, Department of Treasury, was to assess the effectiveness* of the Department's general controls over access to its mainframe information systems.

Audit Scope

Our audit scope was to examine the information processing and other records of the Department of Treasury's automated information systems. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of the Department's information processing and other records primarily for the period October 1999 through March 2001. Our work was performed between October 2000 and June 2001. In addition, in January 2003, we performed a limited follow-up, consisting primarily of inquiries of management, to determine the status of the Department of Treasury and the Department of Information Technology in correcting the conditions cited in this report. To accomplish our audit objective, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We conducted a preliminary review of the Department's information processing function that supports managing changes to production programs and data files, administering access to mainframe systems, and maintaining security for production program and data files. We used this analysis to determine the extent of our detailed analysis and testing.

* *See glossary at end of report for definition.*

2. Detailed Analysis and Testing Phase

We performed an assessment of internal control* pertaining to: (a) controls over the changes to mainframe production data and application programs, and (b) control over access to agency mainframe information systems. Specifically, we assessed:

a. Effectiveness of Change Controls:

We reviewed Department policies and procedures for managing program and data changes.

We selected program and data changes and verified appropriate authorizations and approvals.

We evaluated the effectiveness of Department controls to ensure approved changes are placed into production.

b. Effectiveness of Mainframe Information System Access Controls:

We reviewed and assessed the Department's policy and procedures for managing access to mainframe information systems.

We selected and tested individual access rights to the Department's single business tax system*; sales, use, and withholding system*; individual income tax system*; system utilities; databases; and data and application code files to verify that access was authorized in accordance with Department policy.

We assessed the effectiveness of the Department's controls over access to its mainframe information systems.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

** See glossary at end of report for definition.*

4. Follow-Up Subsequent to the End of Fieldwork

   In January 2003, we inquired of the Department and the Department of Information Technology (DIT) their status in addressing the findings in this report. Based on these inquiries, we determined that the Department and DIT had made improvements in the internal control over information systems; however, action was still required to fully correct the conditions cited in the report. The Department and DIT expect to be in full compliance by September 30, 2003.

Agency Responses and Prior Audit Follow-Up

Our audit report contains 6 findings and 6 corresponding recommendations. The agency preliminary responses indicated that the Department of Treasury agreed with the findings and has partially complied or will comply with the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require the Department of Treasury to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

The Department had not complied with the one prior audit recommendation included within the scope of our current audit. We repeated that prior audit recommendation in this report.

COMMENT, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF ACCESS CONTROLS

COMMENT

Background: The Department of Treasury has developed and operates large complex information systems to manage the processing of numerous personal and business related taxes. These include sales, use, and withholding taxes; individual income tax payments and refunds; and single business tax payments and refunds. The Department's information systems facilitate the processing of over $18 billion a year in tax revenue collections and over $1 billion in tax refund payments.

Audit Objective: To assess the effectiveness of the Department's general controls over access to its mainframe information systems.

Conclusion: The Department's general controls over access to its mainframe information systems were not effective. Our assessment disclosed six material conditions* related to comprehensive information systems security program, organizational controls, access to system account, access to Department information system files, access to tax systems, and program and data change controls.

As a result, there was a significant risk that the Department's system of internal control could not prevent or detect unauthorized access to or use of confidential taxpayer information or the execution of fraudulent financial transactions.

During our audit fieldwork, we reported to Department management the detailed results of our review. This report summarizes the material control conditions we identified and recommendations we made. It also reflects follow-up on previously reported weaknesses.

** See glossary at end of report for definition.*

FINDING

1. Comprehensive Information Systems Security Program

The Department had not established a comprehensive information systems security program.

A comprehensive security program begins with the appointment of an executive level information security officer. The security officer is then given the responsibility and authority to implement information security policies, standards, and operating procedures for safeguarding all information systems resources. The security program is developed based on the results of comprehensive and periodic risk assessments.

The lack of a comprehensive security program contributed to the following material control conditions:

a. The Department had not established effective organizational controls to support its critical information systems (Finding 2).

b. The Department had not controlled access to its critical production system account (Finding 3).

c. The Department had not established effective access controls to its mainframe information system files (Finding 4).

d. The Department had not established effective access controls to its production tax and other information systems (Finding 5).

e. The Department had not established effective program and data change controls (Finding 6).

Without a comprehensive security program, management cannot ensure that the Department's internal control is operating as intended and that sensitive information will remain confidential.

Our audit again found that the Department had not taken steps to establish an effective and comprehensive information security program. We first reported on this issue in our prior audit of the Department's automated information systems

dated June 2000. The agency responded that it would establish a comprehensive information systems security program by September 30, 2001. However, we noted that the Department had made little progress in developing a security program.

RECOMMENDATION

WE AGAIN RECOMMEND THAT THE DEPARTMENT ESTABLISH A COMPREHENSIVE INFORMATION SYSTEMS SECURITY PROGRAM.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation. With Executive Order No. 2001-03, the Governor created the Department of Information Technology (DIT). The Department informed us that in June 2002, the director established the Office of Security and Disaster Recovery and appointed the first chief enterprise security officer who reports directly to the State Chief Information Officer. The Department also informed us that, since then, the chief enterprise security officer and his staff performed a rapid risk assessment and published the Secure Michigan Initiative, which compiles:

- Primary vulnerabilities within all State departments;
- Six immediate strategies that mitigate those vulnerabilities;
- Many other quick-hit, low-cost remedies to improve the security of the State's data and systems; and
- Data that will help direct each department to target its own weaknesses.

The Department appointed a security officer in August 2002. The Department's security officer will develop security policies and guidelines supportive of the Statewide requirements and compliant with Department statutes and regulations by September 2003.

FINDING

2. Organizational Controls

The Department had not established effective organizational controls to support its critical information systems.

During our audit, we noted that the cause of many of our audit findings were in part related to incompatible job assignments, critical functions not assigned, or insufficient expertise in control standards and techniques and information security. We noted the following weaknesses in organizational controls:

a. Management had assigned incompatible job functions to information technology (IT) development staff*. For internal control purposes, functions are considered to be incompatible if their performance by one person places that person in a position to both commit and conceal fraud or error.

   IT development staff were granted inappropriate access and responsibilities, such as correcting data errors, managing program code libraries, administering security and access to the job scheduling utility, and using the Department production system account to access production resources. These functions should be assigned to IT operational support and security functions.

   This has resulted in material control weaknesses throughout the IT development staff function that adversely affect management's ability to maintain the integrity of the Department's information systems.

   The Department should reassign IT operational support and security functions to individuals independent of IT development.

b. The Department had not assigned responsibility for maintaining the security of the Department's databases, data, and program code files. Consequently, the Department cannot ensure that the integrity and security of the Department's databases, data, and program code files are maintained.

* *See glossary at end of report for definition.*

c. The Department did not put in place control standards to effectively manage its information systems resources.

Generally accepted IT control objectives and standards provide a practical framework for identifying, understanding, assessing, and implementing IT controls. The identification and selection of suitable controls are critical to the cost effective management of risk stemming from the use of IT.

Adopting generally accepted IT control objectives and standards provides the Department with the means to comply with the Management and Budget Act (Sections 18.1483 - 18.1489 of the *Michigan Compiled Laws).*

The material conditions identified in the Department's internal control were a result of two primary factors. First, there was a basic lack of understanding and appreciation for generally accepted IT control objectives and standards. Second, there was an overriding concern by the Department that any controls over IT development staff would adversely hinder their ability to service and support business needs. This second factor occurred without first assessing the risk to critical and sensitive Department information systems or financial assets. Consequently, the Department accepted an unknown level of risk without determining what level of risk was tolerable.

The Department should adopt and implement generally accepted IT control objectives and standards as a means of managing risk to its information system resources and ensuring the confidentiality of taxpayer records.

d. The Department lacked sufficient technical training to effectively manage its information systems security needs.

The integration of Department information system security needs with its mainframe security system is highly complex. There are numerous access control systems and just as many different technologies involved in providing security to the Department's mainframe information system resources. These access control systems include the mainframe's file system, database management system, user account system, job scheduling system, program change control system, and transaction control system. The interrelationships

of these various access control systems serve to make overall information security highly complex and difficult to administer.

This highly complex environment requires that the Department assign individuals to information security who possess and maintain the needed knowledge, skills, and ability to effectively manage information security. Without a comprehensive and detailed understanding of the technologies, the Department's information security function will not effectively maintain security over critical information resources.

RECOMMENDATION

We recommend that the Department establish effective organizational controls to support its critical information systems.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve further compliance by June 2003. Both the Department and DIT will work together to ensure that appropriate organizational controls are put in place. Both the Department and DIT expressed concern that budget limitations may hinder their efforts to provide needed training to IT security and other department employees.

FINDING

3. Access to System Account

The Department had not controlled access to its critical production system account.

One of the primary means of controlling access to mainframe information resources is by assigning ownership of the resource. The State's mainframe processing center (Data Center Operations) establishes a unique production system account for each State agency that it serves. Agencies use their production system account to control access to their production resources. It is the responsibility of each State agency to protect information resources and control access to the production system account.

Access to the production system account must be restricted and closely monitored. Access to this account should be limited to operational support staff that are responsible for scheduling production jobs.

Our review of access to the Department production system account disclosed that it was not restricted to operational support personnel. Further, the Department had not established effective controls to administer access to a critical job-scheduling utility.

Access to the production system account can be used to gain unauthorized access to critical Department information resources that may go undetected.

RECOMMENDATION

We recommend that the Department control access to the critical production system account.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and will comply with the recommendation by April 30, 2003. Both the Department and DIT will work together to control access to critical production system accounts.

FINDING

4. Access to Department Information System Files

The Department had not established effective access controls to its mainframe information system files.

The Department stores thousands of files on the State's mainframe computer system. These files support the Department's major tax systems as well as financial and other information systems. We reviewed the access controls for these files and identified material control conditions that prevent the Department from maintaining the integrity and confidentiality of its information systems:

a. The Department had not secured its 14 mainframe production database files from unauthorized access at the operating system level. We identified inappropriate access rights granted to nonoperational support staff and to another State agency's production system account.

b. The Department had not established effective access controls over its mainframe application files.

These files contain application data, program code, and process rules. Our analysis of both production and development files indicates that approximately 4,700 Department files were not properly secured. These files are critical to maintaining the integrity of the Department's information systems and may contain confidential program logic or taxpayer information.

The Department of Management and Budget (DMB) Administrative Guide procedure 1310.02 requires that production programs and data files be protected from unauthorized access. In addition, Department files stored in the development environment must also be protected because confidential business rules or taxpayer information could be disclosed or unauthorized code or data could be introduced into production information systems from the development environment.

RECOMMENDATION

We recommend that the Department establish effective access controls to its mainframe information system files.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve full compliance by September 30, 2003. Both the Department and DIT will work together to establish effective access controls to department mainframe information systems files.

FINDING

5. Access to Tax Systems

The Department had not established effective access controls to its production tax and other information systems.

A basic management objective for any organization should be the protection of its information systems and critical data from unauthorized access. Organizations accomplish this objective in part by establishing controls that limit access to only

authorized users. Our review of the Department's efforts to control access to its major tax information systems disclosed:

a. The Department's information security policy and procedures were not complete.

   The Department had not developed written policy and procedures that defined how access was to be granted, who should be allowed access, and the risks associated with granting certain access rights to the individual income tax system.

   DMB Administrative Guide procedure 1310.02 states that security requirements and procedures must be documented and approved by management for each application system.

   In addition, the Department had not established written policies and procedures for monitoring the privileged activity of its security administrator and security managers. Privileged activity includes setting up security administrators and usercode and access rights managers and granting access to high-risk transaction code lists.

   The Data Center Operations security system framework defines the responsibility of the agency security administrator to establish internal procedures for computer security and monitoring policies.

b. The Department had not implemented an effective audit trail to detect abuse or illegal acts of individuals with access to taxpayer information:

   (1) The Taxpayer Bill of Rights states that access to confidential information shall be restricted to Department employees who have a need to access the information to perform their duties. A Department employee shall not disclose confidential information to another Department employee, except as needed to perform duties.

   Section 205.28(1)(f) of the *Michigan Compiled Laws* states that an employee or authorized representative shall not willfully inspect any tax

return or information contained in a tax return unless it is appropriate for the proper administration of a tax law administered under this act.

In order to be able to track individuals accessing confidential taxpayer information, the Department's disclosure officer in March 1999 requested the development of an audit tracking system that would monitor transactions and maintain a chronological record of the system or application activities. The disclosure officer noted that because all tax return information is considered confidential, the tracking system should track users on a record-by-record basis. In addition, in October 1999, the Internal Revenue Service made a similar recommendation to the Department in a review of the Department's information security procedures.

During our audit, the Department informed us that it had not established plans to implement the disclosure officer's request nor the IRS' recommendation.

(2) The Department had not developed an effective method to monitor payment transactions in order to identify unusual transactions requiring further follow-up. The development of a monitoring process would reduce the risk of fraud or inappropriate use of taxpayer information.

c. The Department had not assessed the risks related to transactions used to access the Department's information systems.

Risk assessments are important because they help ensure that significant threats and vulnerabilities are identified and considered when decisions are made regarding which risks to accept and which to mitigate through security controls.

d. The Department granted IT development staff extensive and inappropriate access to the Department's tax and other information systems.

It is a generally accepted control objective to restrict IT development staff's access to production information resources. The primary reason is that these individuals possess a detailed understanding of the information system as well

as the controls over those systems. Granting these individuals access and the ability to administer access creates a high risk that an individual could commit a fraudulent or unauthorized transaction and conceal it.

Without effective access control to production application systems, the Department cannot maintain the integrity of confidential taxpayer records and critical financial records.

RECOMMENDATION

We recommend that the Department establish effective access controls to its production tax and other information systems.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve full compliance by June 30, 2003. Both the Department and DIT will work together to establish effective access controls to its tax and other information systems.

FINDING

6. Program and Data Change Controls

The Department had not established effective program and data change controls. Our review disclosed:

a. The Department's program change control process did not ensure that appropriate security was maintained over application program code files.

   We noted weaknesses in the controls that allowed nonoperational support staff unrestricted, unmonitored, and unaccountable access to application code files. This environment creates a greater risk that programs and program modifications are not properly authorized, tested, and approved. Effective controls also help prevent security features from being turned off and processing irregularities or malicious code from being introduced.

b. The Department had not established controls over changes made to production data.

We noted that data corrections were not assigned to individuals independent of the systems development function. As previously noted in Finding 3, nonoperational support staff were granted extensive access rights to the production system [account] and job-scheduling utility. Further, the Department management did not monitor changes made to production databases and data files.

This environment does not provide Department management with sufficient control to reduce the risk of unauthorized data changes to a reasonable level.

The Department should establish clear and separate assignments of responsibility and accountability for planning, managing, and controlling changes to data in its information systems. Management should approve all data changes and controls should be in place to ensure that only authorized changes are made to the Department production databases and data files. The Department's internal auditor should review critical job assignments to ensure that an appropriate separation of critical duties is established.

RECOMMENDATION

We recommend that the Department establish effective program and data change controls.

AGENCY PRELIMINARY RESPONSE

The Department agreed with the finding and informed us that it has partially complied with the recommendation and will work to achieve full compliance by June 30, 2003. Both the Department and DIT will work together to establish effective program and data change controls.

Glossary of Acronyms and Terms

Data Center Operations (DCO)	The State's consolidated data center, which is now part of the Department of Information Technology.
DIT	Department of Information Technology.
DMB	Department of Management and Budget.
effectiveness	Program success in achieving mission and goals.
efficiency	Achieving the most outputs and outcomes practical with the minimum amount of resources.
individual income tax system	An information system used to process an individual's tax return and payment or refund of individual income tax.
internal control	The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.
IT	information technology.
IT development staff	Computer programmers, systems analysts, and other persons responsible for developing business application systems.
ITSD	Information Technology Services Division.

material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
mission	The agency's main purpose or the reason that the agency was established.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
sales, use, and withholding system	The information system used to account for taxpayers' payments of the State's sales tax, use tax, and individual income tax withholding.
single business tax system	The information system used to administer the collection of the State's single business tax. The single business tax is the only general business tax levied by the State. It was enacted in 1976 to replace seven business taxes, including the corporate income tax.